7.3.5 Legal

The legal department (Legal) is involved in many areas of information protection. Rank each area from 0 to 10 then sum up the grouped ratings, sum them in the grand total line and divide by 11 for a rating.

7.3.5.1 Regulatory

Issue	Rate
Legal staff have expertise in information protection laws and regulations for all jurisdictions affecting the enterprise.	
Outside legal experts are engaged to assist in regulatory issues.	
Policy requires that all legal regulations be followed unless a written exception is given by top management.	
All regulations not excepted by top management in writing are followed at all times.	
Regulations regarding encryption are followed even if the costs of alternative protection is high.	
A list of specific regulations is provided to the CISO by Legal and matches the CISO expectations.	
Legal provides written guidance to the CISO on how these regulations are to be followed.	
When there is a dispute about regulatory compliance, Legal gets a written ruling from regulators.	
Add the ratings and divide by 8	

7.3.5.2 Civil

Issue	Rate
All published policies are scrupulously followed to avoid punitive damages associated with failure to follow policies.	
Legal review of protection issues is ubiquitous.	
Legal informs the CISO of civil issues associated with all aspects of the protection program.	
Legal is contacted as a matter of course when any information protection incident occurs.	
Add the ratings and divide by 4	

7.3.5.3 Criminal

Issue	Rate
Criminal statutes are well understood by management responsible for making information protection decisions.	
Potentially serious negative consequences of information technology failures are accurate in annual reports.	
Financial records are adequately protected to assure that no serious negative consequences can occur as a result of reasonably anticipatable event sequences.	
Due diligence requirements are met or rapidly mitigated with respect to the information protection program.	
Add the ratings and divide by 4	

7.3.5.4 Notice

Issue	Rate
Legal defines notice requirements associated with all aspects of information protection.	
Notice requirements are met in all information systems.	
Notice of trade secrets, copyrights, and patents is given.	
Users are notified appropriately on first access to systems.	
Add the ratings and divide by 4	

7.3.5.5 Intellectual property

Issue	Rate
Legal specifies requirements for all intellectual property protection.	
Trade secrets are protected per Legal requirements.	
Trade secrets of other entities are protected per Legal requirements.	
Patents are protected per requirements specified by Legal.	
Patents of other entities are protected per Legal requirements specified.	
Copyrights are protected per requirements specified by Legal.	
Copyrights of other entities are protected per Legal requirements.	
Other intellectual property is protected as specified by Legal.	
Add the ratings and divide by 8	

7.3.5.6 Contracts

Issue	Rate
All contract terms pass through Legal before signatures may be affixed and contracts closed.	
Contracts and enforcement requirements relating to customer information is specified by Legal.	
Contracts and enforcement requirements relating to vendor information is specified by Legal.	
Peering agreements associated with financial and health-related information meet regulatory requirements.	
Legal specified protections associated with peering agreements are carried out properly.	
Safe harbor agreements are in place for international contracts.	
Safe harbor agreements are operated as specified by Legal.	
Contracts for all external connections are specified and approved by Legal.	
Contract terms for external connections provide adequate protection for internal systems.	
Contracts prohibit override of control requirements by anyone unless approved in writing by top management.	
All existing contracts have been reviewed for information protection requirements and updated to meet them.	
Legal does periodic reassessments of regulatory requirements for all contracts to reflect changes.	
Add the ratings and divide by 12	

7.3.5.7 Liability

Issue	Rate
Liability issues associated with holding information of all types have been examined by Legal.	
Liability issues associated with systems that interact with third parties have been reviewed by Legal.	
Liability issues associated with actions of employees with access to third party information have been reviewed by Legal.	

Issue	Rate
Liability issues associated with harm caused to other systems by faulty or insecure systems of the enterprise have been examined by Legal.	
Legal has provided guidance on reasonable, prudent, necessary, and appropriate protection to meet due diligence standards with respect to these liabilities.	
Liability issues associated with all other aspects of the information protection program were examined and approved in writing by Legal.	
Liability requirements are regularly reviewed by the legal department and written approvals or mitigation requirements are given each period.	
Add the ratings and divide by 7	

7.3.5.8 Jurisdiction

Issue	Rate
Legal tracks laws related to the information protection function in all relevant jurisdictions.	
Specific jurisdictional requirements are provided by Legal to the CISO for implementation.	
Adequate funding is available to meet these requirements.	
Legal coordinates all issues that cross jurisdictional boundaries and involve legal matters.	
Add the ratings and divide by 5	

7.3.5.9 Investigations

Issue	Rate
Investigations are always controlled by Legal.	
Worker sanction processes follow Legal requirements.	
Legal approves all worker sanctions.	
Employee rights are protected by Legal in investigations.	
Legal determines when to call in outside investigators.	
Legal determines when authorities are to be called in.	
Legal is responsible for external liaison in all investigative matters.	
Add the ratings and divide by 7	

7.3.5.10 Chain of Custody

Issue	Rate
Chain of custody issues are addressed in processes that could ultimately lead to court cases.	
Legal identifies those cases that require chain of custody coverage as part of their investigative decision process.	
Legal provides guidance on chain of custody issues for all relevant jurisdictions.	
Legal notifies those responsible for retention of data of all retention requirements associated with legal proceedings so that data can be retained per judicial orders.	
Legal notifies those with custody when information no longer must be retained for legal purposes.	
Legal mandates data retention times via policy.	
Legal mandates data destruction times via policy.	
Add the ratings and divide by 7	

7.3.5.11 Evidential

Issue	Rate
Legal mandates integrity and accuracy requirements for business records used in legal matters.	
Legal determines expert witness selection from within the enterprise and prepares expert witnesses for testimony	
To meet business records exceptions, legal reviews and approves what records must be generated or not generated in the normal course of business.	
Legal receives and processes preservation orders for evidence and secures that evidence for legal purposes.	
Legal is responsible for assuring that destruction meets all legal requirements including retention requirements.	
Add the ratings and divide by 5	

7.3.5.12 Forensics

Issue	Rate
Legal supervises all forensics efforts.	
Legal is responsible for seeking outside forensics experts when required.	
Legal is responsible for setting internal standards for forensic data processing including identification, collection, preservation, analysis, and presentation of digital forensic evidence.	
Add the ratings and divide by 3	

7.3.5.13 Roll-up

Area	Issue	Rate
TOTAL	Add all the total lines and divide by 11	

Ratings here are based on pre-compliance reviews. Compliance efforts typically put companies into the excellent range.

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	6	5	7	9.5